UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,042	05/06/2004	Eugene Thomas Bond	16379US01	6856

23446 7590 07/21/2011

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER
HOEL, MATTHEW D

ART UNIT	PAPER NUMBER
3714	

NOTIFICATION DATE	DELIVERY MODE
07/21/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mhmpto@mcandrews-ip.com

Office Action Summary	Application No.	Applicant(s)	
	09/720,042	BOND, EUGENE THOMAS	
	Examiner	Art Unit	
	MATTHEW D. HOEL	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *68-87,95,97-100,102 and 103* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *68-87,95,97-100,102 and 103* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

3. Claims 68 to 87, 95, 97 to 100, 102, and 103 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alcorn, et al. (U.S. patent 5,643,086 A) in view of Davis (U.S. patent 5,539,828 A) and Ohno (U.S. patent 5,355,413 A).

1. As to Claim 68: Alcorn discloses all of the limitations of Claim 68, but lacks specificity as to an external authentication agent apparatus and a transmitted authentication algorithm. Alcorn teaches a system for verifying at least one digital medium in a gaming machine (Abst.), said system comprising: an authentication agent, wherein said authentication agent is external to said gaming machine and further wherein said authentication agent (external gaming authority, 2:27-32, 3:13-21, 6:47-

56): transmits verification information to said gaming machine; receives from said gaming machine an outcome of said verification; compares said received outcome with an expected outcome; and authenticates said gaming machine if said received outcome matches said expected outcome (Figs. 4 & 5; 3:35-55, 4:49-58, 8:38-52). Alcorn teaches an authentication program stored on ROM 29 (Fig. 2, 7:16-19), comprised of message digest program 32, decryption program 33, and decryption key 34 (Fig. 3, 7:26-40). Alcorn teaches verifying the content of ROM 29 which comprises a plurality of files as claimed, which would include its authentication program (8:39-53, contents of ROM 29 may be verified with hash function stored securely such as with a gaming commission; this verification may be carried out on demand at any time, such as over the network, 8:8:53-62, also 3:3:15-20 & 4:49-53).

2. Davis, however, teaches an *external* authentication agent apparatus (7:25-55, describing the method of Fig. 8). Davis teaches a remote system generating a challenge (step 330, Fig. 8); transmitting a challenge to the hardware agent system (step 335, Fig. 8); the hardware agent encrypting with a private key its response and transmitting the response to the remote agent, or receiving by the remote agent an outcome of the verification algorithm (steps 340, 345, and 350, Fig. 8); comparing the received outcome with the expected outcome (step 355, Fig. 8); and authenticating the hardware agent system (step 360, ensuring that communications are secured, Fig. 8). It would have been obvious to one of ordinary skill in the art at the time of invention to have applied the verification scheme of Davis to the gaming system of Alcorn. Alcorn teaches an external authentication agent (gaming commission, 8:54-62), which is able

to verify the contents of any of the memory devices on a gaming machine at any time via a remote request over the network; the gaming commission has a custodial version of the memory contents in its custody, so it is able to verify the results of any verification algorithm sent back to it by a gaming machine (8:38-53, 3:13-20). Alcorn also teaches a private key stored custodially by a third party used for verifying memory contents encrypted using the key and decrypted using a public key. This modification would allow the authentication agent's (gaming commission's) authentication agent apparatus to send an algorithm to the gaming machine over the network, verify the contents of the gaming device's memory devices using the verification algorithm, and compare the result of the verification of the gaming device's memory contents with the custodial version held by the gaming commission. Such a modification in which the Alcorn's ROM 29 containing the authentication program is remotely verified by the gaming commission (Alcorn, 8:38-62) is very similar to the way the ROM 29 with the authentication program is able to verify using encryption the contents of the gaming machine's mass storage, which may be stored in a network drive (Fig. 5, 8:1-25, 6:47-57). Both aspects of Alcorn are remote authentication via encryption of memory devices over a network. Alcorn specifically teaches generating a hash from the contents of ROM 29 and comparing it with the custodial version held by the gaming authority (8:38-53); this could be done by the gaming commission sending a key to the gaming device, the key not being known to the gaming device until it is received, the gaming device generating a hash message of ROM 29's contents and sending them back to the gaming commission, and the gaming commission comparing the hash

message to its own custodial version of ROM 29. This modification would have the advantage of enabling the gaming commission to remotely verify the contents of ROM 29 which contains the program used to verify the other memory contents of the gaming machine, by using a verification algorithm which is not known to the gaming device until the time of verification; this would have the advantage of preventing any unauthorized modifications to the authentication program in ROM 29 since the algorithm will not be known in advance, and the verification process could happen at any time for any reason.

3. Ohno, however, teaches an authentication algorithm transmitted from one device to another (Fig. 15, transmission of random number 142, is encryption algorithm received? yes/no 143, encryption algorithm is loaded 144, authentication process 145). This is in reference to the transmission unit 27 and IC card 13 of Fig. 14 (8:34-54): "In this embodiment, after the IC card 13 generates a random number (R) (step 142), the transmission unit 27 transmits the encryption algorithms (f'1) (g'1) to the IC card 13 (step 143). The IC card 13 loads the encryption algorithms (f'1)(g'1) in either the areas 3-a and 3-b of RAM 3 or empty areas 5-i and 5-j of the data memory 5 (step 144). Thereafter, the same authentication operation as that executed in the previous embodiments is performed (step 145). Transmission of the encryption algorithms from the terminal unit to the IC card prior to the authentication process can be applied to each of the previous embodiments." That an encryption algorithm will have a plurality or sequence of steps is evidenced by Hershey, et al. (U.S. patent 5,239,584 A, 1:48-52). It would have been obvious to one of ordinary skill in the art at the time of invention to have applied the transmission of the authentication algorithm

over the network as taught by Ohno to the combination of Alcorn and Davis. Alcorn teaches an authentication program stored on ROM 29 (Fig. 2, 7:16-19), comprised of message digest program 32, decryption program 33, and decryption key 34 (Fig. 3, 7:26-40). Alcorn suggests the desirability of verifying the content of ROM 29, which would include its authentication program (8:39-53, contents of ROM 29 may be verified with hash function stored securely such as with a gaming commission; this verification may be carried out on demand at any time, such as over the network, 8:8:53-62, also 3:3:15-20 & 4:49-53). The gaming commission would necessarily have an authentication apparatus such as that suggested by Davis to generate such an algorithm. The advantage of this modification would be to transmit to the gaming device an authentication algorithm pertaining to encryption instead of merely a challenge/response query, making the authentication process more secure as the gaming device would never have the algorithm for authenticating ROM 29 stored locally, as it would only be known by the gaming commission. The local gaming device would thus only receive this authentication algorithm at the time it is used; since the algorithm would not be stored locally, it would be extremely difficult to tamper with the gaming device undetected.

4. As to Claim 75: Alcorn teaches method for verifying at least one digital medium (Abst., Fig. 1) in a system including gaming machine and an external authentication agent (external gaming authority, 2:27-32, 3:13-21, 6:47-56), said method comprising: transmitting a verification algorithm to said gaming machine from said external authentication agent to said gaming machine; deriving an outcome of said verification

algorithm by execution thereof; comparing said derived outcome with an expected outcome; and authenticating said gaming machine if said derived outcome matches said expected outcome (play permitted if authenticated, Figs. 4 & 5). Receiving the outcome from the gaming machine is addressed in the rejection of Claim 68. The new limitations of Claim 75 are addressed above regarding Claim 68.

5. As to Claim 79: Alcorn teaches gaming device comprising: a gaming controller (Abst., Fig. 1); a data storage device storing data files and data corresponding to a valid verification signature (Fig. 2); an apparatus for loading data external from said gaming machine to said storage device, said apparatus transmitting an authentication agent (external gaming authority, 2:27-32, 3:13-21, 6:47-56); and a processor to process said authentication agent to derive a verification signature and compare said derived signature to said valid signature (Figs. 4 & 5). The new limitations of Claim 79 are addressed above regarding Claim 68.

6. As to Claim 80: Alcorn teaches method for presenting at least one game to a player at a gaming machine (Abst., Fig. 1; player permitted to play or not, Figs. 4 & 5), said method comprising: storing at least one of program code and program data in a digital medium (Figs. 1 & 2); transmitting via a communication link at least one of a program code or program file data and data corresponding to a verification algorithm to said gaming machine from an authentication agent (external gaming authority, 2:27-32, 3:13-21, 6:47-56); processing said verification algorithm to derive an outcome and comparing said outcome to one of an authorized outcome stored in said digital medium or transmitted with said algorithm and authorizing said transmitted program code or

program file data if said derived and stored outcomes compare (Figs. 4 & 5). Receiving the outcome from the gaming machine is addressed in the rejection of Claim 68. The new limitations of Claim 80 are addressed above regarding Claim 68.

7. As to Claim 95: Alcorn teaches a system for monitoring a gaming machine (Abst., Fig. 1), said system comprising: a regulating agent for monitoring at least a portion of said gaming machine, wherein said regulating agent generates a request for an authentication agent (external gaming authority, 2:27-32, 3:13-21, 6:47-56), and wherein said authentication agent is configured to: compare a received outcome from a verification algorithm at said gaming machine with an expected outcome; and authenticate said gaming machine if said received outcome matches said expected outcome (Figs. 4 & 5). Receiving the outcome from the gaming machine is addressed in the rejection of Claim 68. The new limitations of Claim 95 are addressed above regarding Claim 68.

8. As to Claim 69: Alcorn teaches the external agent prompting the gaming machine to request and execute said verification algorithm for said at least one digital medium and enrolls said gaming machine when said received outcome matches at least one of a set of predetermined criteria (game play permitted if match exists, Fig. 5, Alcorn).

9. As to Claim 70: Alcorn teaches the request and execution of said verification algorithm being carried out based on at least one of a request of said gaming machine, a request of a player of said gaming machine, a request of an authorized agent, and upon a randomly or periodically scheduled event (Alcorn, external gaming commission, 3:22-33).

10. As to Claim 71: Alcorn teaches a data structure configured to historically store said received outcome (Alcorn, log of game play, credits, diagnostic information, 6:20-26).

11. As to Claim 72: Alcorn teaches the verification algorithm comprises the verification signature (Alcorn, Figs. 4 & 5).

12. As to Claim 73: Alcorn teaches a processor configured to process said verification algorithm to determine at least one of corruption of said at least one digital medium and tampering with said at least one digital medium (unalterable ROM, authentication of Figs. 4 & 5 is thus checking for tampering, 2:35-41, Alcorn).

13. As to Claim 74: Alcorn teaches the authorization agent is remote to said gaming machine and further comprising a communication link between said authorization agent and said gaming machine for transmission of said verification algorithm to said gaming machine (Alcorn, 3:13-33).

14. As to Claim 76: Alcorn teaches prompting said gaming machine to request and execute said verification algorithm for said at least one digital medium and enrolling said gaming machine when said received outcome matches at least one of a set of predetermined criteria (game play permitted if match exists, Fig. 5, Alcorn).

15. As to Claim 77: Alcorn teaches requesting and executing said verification algorithm based on at least one of a request of said gaming machine, a request of a player of said gaming machine, a request of an authorized agent, and upon a randomly or periodically scheduled event (Alcorn, external gaming commission, 3:22-33).

16. As to Claim 78: Alcorn teaches storing any received outcome from a gaming machine for recollection thereof (Alcorn, digests transmitted to gaming commission for audit purposes, 8:22-25,54-62).

17. As to Claim 81: Alcorn teaches that a player is unable to play said at least one game until receipt of said authentication result (Alcorn, Abst.; 8:22-26).

18. As to Claim 82: Alcorn teaches comprising requesting said authentication result upon a player attempting to execute a game (Alcorn, Fig. 5, 8:1-25, authorization routine called).

19. As to Claim 83: Alcorn teaches providing at least one of program code and program data as a game configured for downloading to said gaming machine, said gaming machine requesting said authentication result upon download of a game to said gaming machine (Alcorn, authentication done when data downloaded to game device, 3:13-33; preparation phase, 2:42-57).

20. As to Claim 84: Alcorn teaches an agent external to said gaming machine triggering transmission of said verification algorithm data and at least one of a program code or program file data (Alcorn, external gaming commission, 3:22-33).

21. As to Claim 85: Alcorn teaches registering said outcome for an audit (Alcorn, 8:54-62).

22. As to Claim 86: Alcorn teaches transmitting said verification algorithm data as a verification signature (Alcorn, Figs. 4 & 5).

23. As to Claim 87: Alcorn teaches processing said verification algorithm for identification of at least one of corruption of said at least one digital medium and

tampering with said at least one digital medium (unalterable ROM, authentication of Figs. 4 & 5 is thus checking for tampering, 2:35-41, Alcorn).

24. As to Claim 97: Alcorn teaches the regulating agent is an external agent located remotely from said gaming machine and remotely monitors at least a portion of said gaming machine (Alcorn, remote verification by external agent, 3:13-33).

25. As to Claim 98: Alcorn teaches that the regulating agent monitors all of said gaming machine, and wherein said authentication agent verifies the integrity of said gaming machine (Alcorn, 3:13-33).

26. As to Claim 99: Alcorn teaches the authentication agent being configured to verify that said gaming machine satisfies local gaming regulations (Alcorn, gaming commission audits, 8:54-62).

27. As to Claim 100: Alcorn teaches that the regulating agent monitors software and peripheral devices of said gaming machine (Alcorn, all memory devices in architecture checked, 3:55-67).

28. As to Claim 102: Alcorn teaches that the verification algorithm detects tampering or rigging of software within said gaming machine (Alcorn, 8:1-25).

29. As to Claim 103: Alcorn teaches that the authentication agent authenticates data stored on a digital medium in said gaming machine (Alcorn, 8:1-25, Figs. 4 & 5).

Response to Arguments

Applicant's arguments filed 05-09-2011 have been fully considered but they are not persuasive. Regarding the remarks on pages 1 to 7, In response to applicant's

arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). The examiner believes that Alcorn discloses transmitting a verification algorithm to the gaming machine and receiving the verification algorithm from the gaming machine. The applicant appears to intend the examiner to interpret that structure such as ROM 29 of Alcorn Fig. 2 is stored and executed externally. The applicant previously did not claims what the verification algorithm is. It could have been a hash function (Alcorn, Fig. 4, 41), an encryption program (Alcorn, Fig. 4, 43), a decryption program (Alcorn, Fig. 5, 33), or a message digest program (Alcorn, 32, Fig. 3). Alcorn teaches that the gaming data and unique signature are stored externally (2:27-32). The game data set is only installed on the gaming machine after authentication (2:45-57), so if the gaming data set is stored externally it must receive a signal from the gaming machine before it is loaded onto the gaming machine. The decryption of Alcorn is done with a public key stored in ROM 29 on the gaming device (3:3-6). The game data set on the network is then installed (3:8-12). This will necessarily require a signal from the gaming machine. Quoting from 3:35-55: "From an apparatus standpoint, the first aspect of the invention comprises an electronic casino gaming system for providing authentication of a game data set of a casino type game prior to permitting game play, the system including first means for storing a casino game data set and a signature of the casino game data set, the signature comprising an encrypted version of a unique first abbreviated bit string computed from the casino game data set; second means for storing an authentication program capable of computing a second abbreviated bit string from the casino game data set stored in the first

storing means and capable of decrypting the encrypted signature stored in the first storing means to recover the first abbreviated bit string; processing means for enabling the authentication program to compute an abbreviated bit string from the casino game data set stored in the first storing means and for enabling the authentication program to decrypt the encrypted signature; and means for comparing the computed second abbreviated bit string with the decrypted abbreviated bit string to determine whether a match is present. The first storing means preferably comprises a mass storage device, such as a disk drive unit, a CD-ROM unit or a network storage unit. The second storing means preferably comprises an unalterable read only memory in which the authentication program is stored." The first storing means corresponds to the mass storage unit, and the second storage means corresponds to ROM 29 of Alcorn. The authentication can be conducted locally or externally via a network (4:49-58). This external authentication is used to authenticate ROM 29 in the same manner as ROM 29 authenticates the mass storage unit and the rest of the contents of the gaming machine (8:38-52); in this case the authentication program would necessarily be external to the gaming machine. This can be done for example, by the gaming commission (8:54-62), so the gaming machine would receive a verification algorithm from the external source and send it back to the external authentication agent (9:47-58). On page 14 of the last office action, the examiner was saying that the gaming commission would be able to verify the results of any verification algorithm sent back to it, intending to mean the verification algorithm stored locally as taught in Alcorn with the results being transmitted back to the commision; the examiner was not saying that Alcorn teaches the transmission of an authentication algorithm. The examiner does believe that the transmission of an authentication algorithm would be a minor modification to Alcorn at the time of invention for the following reasons.

30. Davis teaches an external authentication agent apparatus (7:25-55, describing the method of Fig. 8). Davis teaches a remote system generating a challenge (step 330, Fig. 8); transmitting a challenge to the hardware agent system, or transmitting a verification algorithm (step 335, Fig. 8); the hardware agent encrypting with a private key its response and transmitting the response to the remote agent, or receiving by the remote agent an outcome of the verification algorithm (steps 340, 345, and 350, Fig. 8); comparing the received outcome with the expected outcome (step 355, Fig. 8); and authenticating the hardware agent system (step 360, ensuring that communications are secured, Fig. 8). Alcorn teaches an external authentication agent (gaming commission, 8:54-62), which is able to verify the contents of any of the memory devices on a gaming machine at any time via a remote request over the network; the gaming commission has a custodial version of the memory contents in its custody, so it is able to verify the results of any verification algorithm sent back to it by a gaming machine (8:38-53, 3:13-20). Alcorn also teaches a private key stored custodially by a third party used for verifying memory contents encrypted using the key and decrypted using a public key. This modification would allow the authentication agent's (gaming commission's) authentication agent apparatus to send an algorithm to the gaming machine over the network, verify the contents of the gaming device's memory devices using the verification algorithm (most likely an encryption key), and compare the result of the verification of the gaming device's memory contents with the custodial version held by the gaming commission. Such a modification in which the Alcorn's ROM 29 containing the authentication program is remotely verified by the gaming commission (Alcorn, 8:38-

62) is very similar to the way the ROM 29 with the authentication program is able to verify using encryption the contents of the gaming machine's mass storage, which may be stored in a network drive (Fig. 5, 8:1-25, 6:47-57). Both aspects of Alcorn are remote authentication via encryption of memory devices over a network. Alcorn specifically teaches generating a hash from the contents of ROM 29 and comparing it with the custodial version held by the gaming authority (8:38-53); this could be done by the gaming commission sending a key to the gaming device, the key not being known to the gaming device until it is received, the gaming device generating a hash message of ROM 29's contents and sending them back to the gaming commission, and the gaming commission comparing the hash message to its own custodial version of ROM 29.

31. The crux of the matter is that the examiner does not believe that merely transmitting an authentication algorithm from a remote party to a networked gaming device contributes anything patentable over Alcorn, since Alcorn already teaches that the message digest resulting from the hash function used to verify ROM 29 can be transferred over the network back to the casino operator or gaming commission in response to a network-initiated authentication command (3:35-55, 4:49-58, 8:38-52); authentication information, though not a complete algorithm, is already transmitted to the gaming device, the only difference with Aclorn is that the claimed algorithm is a series of instructions. This verification could also be done with a transmitted authentication algorithm comprising a plurality of steps as suggested by Ohno. Ohno teaches an authentication algorithm transmitted from one device to another (Fig. 15, transmission of random number 142, is encryption algorithm received? yes/no 143,

encryption algorithm is loaded 144, authentication process 145). Ohno (8:23-52): "FIG. 14 is a block diagram showing the functional structure of a system including an IC card and a terminal unit used in a fourth embodiment according to the present invention. The fourth embodiment differs from the third embodiment shown in FIG. 10 in that the encryption algorithms f1, g1 are not stored in the data memory 5 of the IC card 13. FIG. 15 is a flowchart showing the operation of the IC card which is executed in the authentication operation between an IC card and a terminal unit in the fourth embodiment of the present invention. ¶ In this embodiment, after the IC card 13 generates a random number (R) (step 142), the transmission unit 27 transmits the encryption algorithms (f'1) (g'1) to the IC card 13 (step 143). The IC card 13 loads the encryption algorithms (f'1)(g'1) in either the areas 3-a and 3-b of RAM 3 or empty areas 5-i and 5-j of the data memory 5 (step 144). Thereafter, the same authentication operation as that executed in the previous embodiments is performed (step 145). Transmission of the encryption algorithms from the terminal unit to the IC card prior to the authentication process can be applied to each of the previous embodiments. ¶ An embodiment intended to improve security regarding a transaction between the IC card and the terminal unit will be described below. In this embodiment, the number of times that transaction is performed is counted, and when that counted value reaches a certain set value, e.g., 100, authentication by another authentication code is conducted." These steps use an encryption algorithm to perform an authentication operation and they are transmitted from one system to another. This is in reference to the transmission unit 27 and IC card 13 of Fig. 14 (8:34-54). That an encryption algorithm will have a plurality or sequence of steps is evidenced by Hershey, et al. (U.S. patent 5,239,584 A, 1:48-52). Alcorn teaches an authentication program stored on ROM 29 (Fig. 2, 7:16-19), comprised of message digest program 32, decryption program 33, and decryption key 34 (Fig. 3, 7:26-40). Alcorn suggests the desirability of verifying the content of ROM 29, which would include its authentication program (8:39-53, contents of ROM 29 may be verified with hash function stored securely such as with a gaming commission; this verification may be carried out on demand at any time, such as over the network, 8:8:53-62, also 3:3:15-20 & 4:49-53). The gaming commission would necessarily have an authentication apparatus such as that suggested by Davis to

generate such an algorithm. The effect of this modification would be to transmit to the gaming device an authentication algorithm pertaining to encryption instead of merely a challenge/response query, making the authentication process more secure as the gaming device would never have the algorithm for authenticating ROM 29 stored locally, as it would only be known by the gaming commission. The local gaming device would thus only receive this authentication algorithm at the time it is used; since the algorithm would not be stored locally, it would be extremely difficult to tamper with the gaming device undetected. The rest of the arguments have been addressed above. The examiner respectfully disagrees with the applicant as to the claims' condition for allowance.

Conclusion

32. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW D. HOEL whose telephone number is (571)272-5961. The examiner can normally be reached on 8:00 A.M. to 4:30 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David L. Lewis can be reached on (571) 272-7673. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. D. H./
Examiner, Art Unit 3714

/DAVID L LEWIS/
Supervisory Patent Examiner, Art Unit 3714